R E P U B L I Q U E F R A N Ç A I S E

INPI
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

BREVET D'INVENTION

CERTIFICAT D'UTILITÉ - CERTIFICAT D'ADDITION

COPIE OFFICIELLE

Le Directeur général de l'Institut national de la propriété industrielle certifie que le document ci-annexé est la copie certifiée conforme d'une demande de titre de propriété industrielle déposée à l'Institut.

Fait à Paris, le 21 DEC. 2000

Pour le Directeur général de l'Institut
national de la propriété industrielle
Le Chef du Département des brevets

Martine PLANCHE

INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE
SIEGE
26 bis, rue de Saint Petersbourg
75800 PARIS cedex 08
Téléphone : 01 53 04 53 04
Télécopie : 01 42 93 59 30
http://www.inpi.fr

ETABLISSEMENT PUBLIC NATIONAL CREE PAR LA LOI N° 51-444 DU 19 AVRIL 1951

INPI
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

26 bis, rue de Saint Pétersbourg
75800 Paris Cedex 08
Téléphone : 01 53 04 53 04 Télécopie : 01 42 94 86 54

BREVET D'INVENTION
CERTIFICAT D'UTILITÉ

Code de la propriété intellectuelle - Livre VI

cerfa N° 11354*01

REQUÊTE EN DÉLIVRANCE 1/2

Cet imprimé est à remplir lisiblement à l'encre noire DB 540 W /260899

Réservé à l'INPI

REMISE DES PIÈCES
DATE 31 JAN 2000
LIEU 75 INPI PARIS

N° D'ENREGISTREMENT NATIONAL ATTRIBUÉ PAR L'INPI 0001199

DATE DE DÉPÔT ATTRIBUÉE PAR L'INPI 31.01.2000

1 NOM ET ADRESSE DU DEMANDEUR OU DU MANDATAIRE À QUI LA CORRESPONDANCE DOIT ÊTRE ADRESSÉE

CABINET BONNET-THIRION
12, avenue de la Grande Armée
75017 PARIS

Vos références pour ce dossier *(facultatif)* BIF114059/FR

Confirmation d'un dépôt par télécopie ☐ N° attribué par l'INPI à la télécopie

2 NATURE DE LA DEMANDE	Cochez l'une des 4 cases suivantes
Demande de brevet	☒
Demande de certificat d'utilité	☐
Demande divisionnaire	☐
Demande de brevet initiale	N° Date / /
ou demande de certificat d'utilité initiale	N° Date / /
Transformation d'une demande de brevet européen *Demande de brevet initiale*	☐ N° Date / /

3 TITRE DE L'INVENTION (200 caractères ou espaces maximum)

Procédé d'exécution d'un protocole cryptographique entre deux entités électroniques.

4 DÉCLARATION DE PRIORITÉ OU REQUÊTE DU BÉNÉFICE DE LA DATE DE DÉPÔT D'UNE DEMANDE ANTÉRIEURE FRANÇAISE	
	Pays ou organisation Date / / N°
	Pays ou organisation Date / / N°
	Pays ou organisation Date / / N°
	☐ S'il y a d'autres priorités, cochez la case et utilisez l'imprimé «Suite»

5 DEMANDEUR		☐ S'il y a d'autres demandeurs, cochez la case et utilisez l'imprimé «Suite»
Nom ou dénomination sociale		OBERTHUR CARD SYSTEMS SAS
Prénoms		
Forme juridique		Société par actions simplifiée
N° SIREN		
Code APE-NAF		
Adresse	Rue	102 Boulevard Malesherbes,
	Code postal et ville	75017 PARIS
Pays		FRANCE
Nationalité		FRANCAISE
N° de téléphone *(facultatif)*		
N° de télécopie *(facultatif)*		
Adresse électronique *(facultatif)*		

INPI
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

BREVET D'INVENTION
CERTIFICAT D'UTILITÉ

REQUÊTE EN DÉLIVRANCE 2/2

Réservé à l'INPI

REMISE DES PIÈCES
DATE
LIEU 31 JAN 2000
75 INPI PARIS
N° D'ENREGISTREMENT
NATIONAL ATTRIBUÉ PAR L'INPI 0001199

DB 540 W /260899

Vos références pour ce dossier : *(facultatif)*		BIF114059/FR
6 MANDATAIRE		
Nom		
Prénom		
Cabinet ou Société		CABINET BONNET-THIRION
N °de pouvoir permanent et/ou de lien contractuel		
Adresse	Rue	12, Avenue De La Grande Armée
	Code postal et ville	750017 PARIS
N° de téléphone *(facultatif)*		01 53 81 17 00
N° de télécopie *(facultatif)*		
Adresse électronique *(facultatif)*		
7 INVENTEUR (S)		
Les inventeurs sont les demandeurs		☐ Oui ☒ Non **Dans ce cas fournir une désignation d'inventeur(s) séparée**
8 RAPPORT DE RECHERCHE		**Uniquement pour une demande de brevet (y compris division et transformation)**
Établissement immédiat ou établissement différé		☒ ☐
Paiement échelonné de la redevance		**Paiement en trois versements, uniquement pour les personnes physiques** ☐ Oui ☐ Non
9 RÉDUCTION DU TAUX DES REDEVANCES		**Uniquement pour les personnes physiques** ☐ Requise pour la première fois pour cette invention *(joindre un avis de non-imposition)* ☐ Requise antérieurement à ce dépôt *(joindre une copie de la décision d'admission pour cette invention ou indiquer sa référence)* :
Si vous avez utilisé l'imprimé «Suite», indiquez le nombre de pages jointes		

10 SIGNATURE DU DEMANDEUR OU DU MANDATAIRE (Nom et qualité du signataire)

Joël ~~BARBIN LE BOURHIS N°92.1010~~
CABINET BONNET-THIRION

VISA DE LA PRÉFECTURE OU DE L'INPI

ADAO

La loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés s'applique aux réponses faites à ce formulaire. Elle garantit un droit d'accès et de rectification pour les données vous concernant auprès de l'INPI.

INPI
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

BREVET D'INVENTION
CERTIFICAT D'UTILITÉ

Code de la propriété intellectuelle - Livre VI

cerfa N° 11235*02

DÉPARTEMENT DES BREVETS

26 bis, rue de Saint Pétersbourg
75800 Paris Cedex 08
Téléphone : 01 53 04 53 04 Télécopie : 01 42 94 86 54

DÉSIGNATION D'INVENTEUR(S) Page N° 1. / 1.
(Si le demandeur n'est pas l'inventeur ou l'unique inventeur)

Cet imprimé est à remplir lisiblement à l'encre noire

DB 113 W / 260899

Vos références pour ce dossier *(facultatif)*	BIF114059/FR
N° D'ENREGISTREMENT NATIONAL	0001199

TITRE DE L'INVENTION (200 caractères ou espaces maximum)

Procédé d'exécution d'un protocole cryptographique entre deux entités électroniques.

LE(S) DEMANDEUR(S) :

OBERTHUR CARD SYSTEMS SAS

DESIGNE(NT) EN TANT QU'INVENTEUR(S) : (Indiquez en haut à droite «Page N° 1/1» S'il y a plus de trois inventeurs, utilisez un formulaire identique et numérotez chaque page en indiquant le nombre total de pages).

Nom		AKKAR
Prénoms		Mehdi-Laurent
Adresse	Rue	17, rue Lafouge,
	Code postal et ville	94250 GENTILLY, France.
Société d'appartenance *(facultatif)*		
Nom		DISCHAMP
Prénoms		Paul
Adresse	Rue	26, rue Saint Laurent,
	Code postal et ville	75015 PARIS, France.
Société d'appartenance *(facultatif)*		
Nom		
Prénoms		
Adresse	Rue	
	Code postal et ville	
Société d'appartenance *(facultatif)*		

DATE ET SIGNATURE(S) DU (DES) DEMANDEUR(S) OU DU MANDATAIRE (Nom et qualité du signataire)	Le 31 Janvier 2000 Joël BARBIN LE BOURHIS N°92.1010 CABINET BONNET-THIRION

"Procédé d'exécution d'un protocole cryptographique entre deux entités électroniques"

L'invention se rapporte à un procédé d'exécution d'un protocole cryptographique entre deux entités électroniques, l'une d'elles étant par exemple, mais non exclusivement une carte à microprocesseur. L'invention concerne plus particulièrement un perfectionnement dudit protocole pour prévenir les "attaques", c'est-à-dire les tentatives de fraude fondées sur l'analyse du matériel en fonctionnement, notamment par le biais de mesures de la consommation de courant pendant l'exécution d'un tel protocole cryptographique provoqué par un fraudeur.

On sait que certaines entités électroniques cryptées, notamment les cartes à microcircuits sont vulnérables à certaines attaques fondées sur l'analyse de certains paramètres pendant une phase de fonctionnement. On dit que les informations peuvent "fuir" à partir d'un calcul fait dans la carte, typiquement l'exécution d'un protocole cryptographique provoqué par le fraudeur en possession de la carte. Les paramètres analysés pendant l'exécution d'un tel protocole peuvent être, typiquement, des différences de temps de calcul ou des radiations électromagnétiques pendant l'exécution du calcul mais surtout la consommation de courant de l'entité électronique dont on cherche à forcer le code.

Ainsi, l'attaque classique consiste à faire exécuter par l'entité électronique tombée en la possession du fraudeur, un certain nombre de protocoles cryptographiques fondés sur des messages quelconques, donc voués à l'échec, mais ayant pour conséquence de faire exécuter chaque fois, par l'entité (la carte à microcircuit) une chaîne d'opérations connue sous l'abréviation DES (Data Encryption Standard) tout en analysant la consommation de courant à chaque exécution dudit DES. Le but de cette attaque est de retrouver la clé secrète de ladite entité. Le DES est, quant à lui, un algorithme bien connu, très largement utilisé actuellement dans le domaine des cartes bancaires ou celui des cartes de contrôle d'accès.

A titre d'exemple, dans le cadre d'une authentification normale entre une entité A, par exemple un serveur et une entité B, par exemple une carte à

microcircuit dans laquelle le DES se trouve programmé, les échanges d'informations entre les deux entités sont les suivants :

- le serveur A demande à la carte B d'envoyer un message, A et B étant supposés être en possession de la même clé.

- B envoie un message quelconque et le garde en mémoire.

- A applique le DES au message en utilisant sa clé et renvoie le résultat à la carte B.

- Parallèlement, la carte B applique le DES au message qu'elle a envoyé au serveur A en faisant usage de sa propre clé. Elle obtient un résultat qui est comparé à celui qui a été élaboré par le serveur A. Si les deux résultats sont identiques, l'authentification est validée.

Par ailleurs, dans le cas d'une fraude, c'est-à-dire dans le cas où le fraudeur dispose de la carte et cherche à déterminer la clé, celui-ci peut connecter la carte à un lecteur par lequel il pourra lui transmettre des messages et la relier à des moyens d'enregistrement de la consommation de courant pendant l'exécution des opérations qu'elle effectue.

A partir de ces moyens simples, le fraudeur constitue un système F qu'il connecte la carte à la place du serveur A.

Le processus est alors le suivant. F demande un message à la carte exactement comme dans le cas de l'initialisation d'une authentification. B envoie ce message. F envoie à B un autre message censé représenter le résultat du traitement par le DES du message envoyé par B. Bien entendu, ce message est erroné. Cependant, B fait intervenir sa propre clé pour exécuter un DES afin d'obtenir un résultat, dans le but de le comparer avec le message (erroné) envoyé par F. Le résultat de cette comparaison est forcément négatif mais le fraudeur a réussi à provoquer l'exécution d'un DES par B. Pendant l'exécution dudit DES, la consommation de courant est détectée et mémorisée.

Si F est en mesure de faire effectuer un certain nombre de DES, dans les mêmes conditions, par la carte B, et de mémoriser à chaque fois les consommations de courant, il est possible de mettre en œuvre une attaque dont le principe est connu. Cette attaque dite "DPA" (Différentiel Power Analysis) permet de reconstituer la clé secrète de l'entité B.

Le document WO 99/63696 vise à contrer des attaques de ce type en réduisant les informations exploitables susceptibles de "fuir" pendant l'exécution des algorithmes. Pour ce faire, il suggère notamment d'introduire des aléas dans les protocoles cryptographiques afin d'augmenter le nombre de cycles nécessaires pour retrouver la clé secrète.

L'invention propose une parade précise à une attaque du genre "DPA" par complémentation aléatoire de certaines opérations du DES.

L'invention s'applique tout particulièrement aux entités utilisant le DES mais elle est applicable aussi, comme on le verra plus loin, à d'autres entités (cartes à microcircuits) utilisant d'autres algorithmes que le DES pourvu que celui-ci soit constitué d'une succession d'opérations possédant certaines propriétés qui seront explicitées plus loin.

Plus précisément, l'invention concerne un procédé d'élaboration d'un protocole cryptographique entre une première entité électronique et une seconde entité électronique susceptible d'attaque, selon lequel un message quelconque est élaboré, à partir duquel une chaîne d'opérations est effectuée par ladite seconde entité, aboutissant à l'élaboration d'un message résultant ou réponse, ladite réponse étant comparée au résultat d'un autre traitement semblable appliqué audit message et effectué par ladite première entité, caractérisé en ce que, au moins à certaines étapes de ladite chaîne d'opérations, ladite seconde entité effectue, soit une opération d'un type choisi, soit la même opération complémentée, le choix dépendant d'une décision aléatoire et en ce que ladite réponse est constituée par le résultat de la dernière opération de ladite chaîne, éventuellement complémenté.

La complémentation peut être réalisée soit octet par octet, en faisant le OU exclusif de l'octet courant aléatoirement avec l'une des deux valeurs hexadécimales 00 et FF, soit bit à bit, en traitant ensemble les huit bits consécutifs de l'octet courant et en faisant le OU exclusif avec un nombre choisi aléatoirement, à chaque octet traité, parmi les 256 valeurs hexadécimales comprises entre 00 et FF.

Parmi les opérations susceptibles d'être complémentées, on peut citer l'opération dite de OU exclusif ou encore une opération de permutation des bits du message ou d'un résultat intermédiaire obtenu en effectuant ladite chaîne

d'opérations, c'est-à-dire, selon l'exemple décrit, après l'exécution d'une opération donnée du DES. On peut encore citer l'opération d'accès indexé à un tableau ou toute opération stable par rapport à l'application de la fonction OU exclusif, notamment l'opération consistant à transférer le message ou un résultat intermédiaire précité, d'un emplacement à un autre, d'un espace de mémorisation.

Selon un mode de réalisation possible, on définit dans ladite seconde entité deux chaînes d'opérations pour le traitement dudit message, l'une des chaînes étant constituée d'une suite d'opérations données et l'autre chaîne étant constituée d'une suite des mêmes opérations complémentées et d'une complémentation finale et on décide de façon aléatoire d'exécuter l'une des deux chaînes d'opérations à chaque réception d'un message provenant de ladite première entité.

Selon un autre mode de réalisation, actuellement jugé préférable, le procédé consiste à utiliser ledit message ou un résultat intermédiaire résultant de l'exécution d'une opération précédente de ladite chaîne, à lui appliquer une nouvelle opération de ladite chaîne, ou cette même opération complémentée, en fonction de l'état d'un paramètre aléatoire associé à cette nouvelle opération, à mettre à jour un compteur de complémentations et à prendre en compte l'état de ce compteur à la fin de l'exécution de ladite chaîne d'opérations pour décider de la configuration finale de ladite réponse.

Selon encore une autre variante avantageuse, le procédé consiste à utiliser ledit message ou un résultat intermédiaire résultant de l'exécution d'une opération précédente de ladite chaîne, à lui appliquer une nouvelle opération de ladite chaîne ou cette même opération complémentée, en fonction de l'état d'un paramètre aléatoire associé à cette nouvelle opération et à transmettre, d'opération en opération, des informations faisant partie desdits résultats intermédiaires, nécessaires à la configuration finale de ladite réponse.

Par ailleurs, on a trouvé que la différence entre le nombre de fois où les opérations sont effectuées de façon normale et le nombre de fois où elles sont effectuées avec complémentation, pendant l'exécution du DES ou analogue, ne doit pas être trop importante pour que le procédé conserve toute son efficacité vis-à-vis de l'attaque décrite ci-dessus. Par conséquent, le procédé est aussi

remarquable par le fait que, pendant qu'on effectue ladite série d'opérations, on calcule la différence entre le nombre de fois où les opérations ont été effectuées de façon normale et le nombre de fois où elles ont été effectuées avec complémentation et en ce qu'on supprime l'aléa sur la décision d'effectuer des opérations de façon normale ou complémentée, pour un certain nombre d'opérations subséquentes, lorsque ladite différence dépasse une valeur prédéterminée, en vue de réduire ladite différence.

L'invention sera mieux comprise et d'autres avantages de celle-ci apparaîtront plus clairement à la lumière de la description qui va suivre, d'un procédé d'exécution d'un protocole cryptographique conforme à son principe, donnée uniquement à titre d'exemple et faite en référence aux dessins annexés dans lesquels :

- la figure 1 est un schéma illustrant une partie de l'exécution d'un protocole cryptographique, plus précisément l'exécution d'un DES programmé selon l'invention ; et

- la figure 2 est un schéma illustrant une autre façon d'exécuter le DES conformément à l'invention.

En considérant plus particulièrement la figure 1, on note que le procédé d'élaboration d'un protocole cryptographique entre deux entités électroniques A et B, qui est partiellement illustré sur le schéma, peut être exécuté dans l'une de ces entités, typiquement dans une carte à microprocesseur B lorsque celle-ci est connectée, par exemple, à un serveur A. Le DES conforme à l'invention est programmé dans la carte à microprocesseur B. Celle-ci renferme également en mémoire une clé secrète K qui est susceptible d'intervenir dans certaines des opérations O_1, O_2, O_3 ...O_n qui s'enchaînent lors de l'exécution du DES. Pendant l'élaboration du protocole cryptographique, la première entité (typiquement le serveur A précité) demande à la seconde entité (la carte B) d'envoyer un message M. Le message généré par B est quelconque ; il est gardé en mémoire dans la carte B. Pendant que A traite ce message avec son propre DES, la carte B applique le DES conforme à l'invention au message M qu'elle a envoyé au serveur A, en faisant usage de sa propre clé K. Dans l'exemple, le DES appliqué dans la carte B comporte deux chaînes d'opérations. Une première chaîne Ch_1 d'opérations O_1, O_2, O_3 ... O_n correspond à un DES classique. La seconde

chaîne Ch_2 d'opérations $\bar{O}_1, \bar{O}_2, \bar{O}_3, \ldots \bar{O}_n$ est constituée de la même succession des mêmes opérations, mais complémentées. Elle s'achève par une complémentation globale C du résultat élaboré à la fin de la dernière opération complémentée $\bar{O}_n$.

En outre, on décide de façon aléatoire d'exécuter l'une ou l'autre des deux chaînes d'opérations à chaque élaboration d'un message quelconque précité. Ce choix aléatoire est symbolisé par un sélecteur S_a interposé entre le message M et chacune des deux chaînes d'opérations. Le positionnement du sélecteur est aléatoire, ce qui signifie que chaque fois qu'un message M doit être traité, l'une ou l'autre des deux chaînes d'opérations Ch_1, Ch_2 est choisie de façon aléatoire.

Si la chaîne non complémentée a été choisie, le résultat donné par la dernière opération O_n constitue la réponse R qui sera comparée à celle qu'aura élaboré le serveur A. Dans le cas où la chaîne des opérations complémentées a été sélectionnée, le résultat de la dernière opération $\bar{O}_n$ est complémenté et constitue la réponse R.

Dans le mode de réalisation de la figure 2, on retrouve un DES programmé conformément au principe de l'invention, c'est-à-dire comportant les opérations habituelles d'un DES : O_1, O_2, O_3 ... O_n ou les opérations semblables complémentées $\bar{O}_1, \bar{O}_2, \bar{O}_3, \ldots \bar{O}_n$. Le message lui-même peut être complémenté, c'est-à-dire utilisé tel quel au début de l'exécution du DES ou sous forme complémentée $\bar{M}$. La clé K intervient pour l'exécution de certaines opérations au moins. Cependant, la sélection des opérations, (c'est-à-dire le choix entre l'opération normale ou sa version complémentée) est décidée de façon aléatoire d'une opération à l'autre. Autrement dit, on utilise le message M ou un résultat intermédiaire résultant de l'exécution d'une opération précédente O_i (ou $\bar{O}_i$), on lui applique une nouvelle opération de la chaîne ou sa version complémentée (c'est-à-dire O_{i+1} ou $\bar{O}_{i+1}$) en fonction de l'état d'un paramètre aléatoire associé à la nouvelle opération. Ce paramètre aléatoire est élaboré par le sélecteur S'_a. Ainsi, en suivant le cheminement de la figure 2, on voit que c'est le message M,

tel quel, qui est utilisé et non son complément $\overline{M}$ (commande 1 générée par S'_a) que c'est l'opération $\overline{O_1}$ qui est sélectionnée (commande 2) puis l'opération $\overline{O_2}$ (commande 3), puis l'opération O_3 (commande 4) et qu'enfin on aboutit à la sélection de l'opération $\overline{O_n}$ (commande n). Le résultat de la dernière opération, en l'occurrence ici $\overline{O_n}$ peut constituer le résultat R ou le résultat $\overline{R}$ complémenté qui sera comparé à un autre résultat élaboré par l'entité A par mise en œuvre de son propre DES. Le choix entre R et $\overline{R}$ est donné par l'état d'un compteur de complémentation C_c alimenté tout au long de l'élaboration du processus par le sélecteur S'_a. Autrement dit, l'état du compteur de complémentation C_c permet de savoir si on doit valider le résultat R ou son complément $\overline{R}$ pour la configuration finale de la réponse à comparer aux calculs de l'entité A.

Il est à noter qu'une variante permet de supprimer le compteur C_c. Il suffit de transmettre, d'opération en opération, des informations faisant partie des résultats intermédiaires et représentant le nombre de fois où une opération du DES a été exécutée sous forme complémentée. Dans ce cas, les résultats intermédiaires transmis d'une opération à l'autre comportent eux-mêmes l'information équivalente à celle que donne in fine le compteur C_c dans le mode de réalisation de la figure 2. Dans ce cas, le dernier résultat intermédiaire donné par l'exécution de l'opération O_n ou $\overline{O_n}$ est ou non complémenté en fonction d'une partie des informations propres qu'il contient. On en déduit la configuration finale de la réponse R.

Revenant à la figure 1 ou 2, on note que le sélecteur S_a ou S'_a est exploité pour calculer la différence entre le nombre de fois où les opérations ont été effectuées de façon normale et le nombre de fois où elles ont été effectuées avec complémentation. Cette différence $\underline{d}$ est mémorisée et actualisée d'opération en opération.

Lorsque la différence dépasse une valeur prédéterminée, ce qui peut réduire l'efficacité du procédé vis-à-vis de l'attaque DPA, on génère un ordre qui inhibe momentanément le sélecteur S'_a. Autrement dit, on supprime l'aléa sur la décision d'effectuer des opérations de façon normale ou complémentée, pour

exécuter un certain nombre d'opérations subséquentes dans le mode (normal ou complémenté) le moins utilisé jusque là. L'aléa est remis en œuvre lorsque la valeur de la différence d a été suffisamment réduite.

Il se trouve que toutes les opérations d'un DES classique permettent la mise en œuvre du procédé selon l'une ou l'autre des variantes qui viennent d'être décrites.

A titre d'exemple, on va mentionner ci-dessous certaines opérations susceptibles d'être complémentées et par conséquent compatibles avec la mise en œuvre du procédé qui vient d'être décrit.

Une opération susceptible d'être complémentée est l'opération dite de OU exclusif.

Une autre opération susceptible d'être complémentée, est une opération connue de permutation des bits du message M ou d'un résultat intermédiaire obtenu en effectuant la chaîne d'opérations. Pour les permutations (simples, compressives ou expansives), on stockera avantageusement le masque permuté en mémoire.

Une autre opération susceptible d'être complémentée est l'opération dite d'accès indexé à un tableau.

Une autre opération susceptible d'être complémentée est le transfert du message ou d'un résultat intermédiaire obtenu en effectuant une opération de la chaîne, d'un emplacement à un autre d'un espace de mémorisation défini dans l'entité B. Pratiquement, on applique de manière aléatoire un masque par OU exclusif à la donnée transférée.

Plus généralement, une opération susceptible d'être complémentée est une opération stable par rapport à l'application de la fonction ou exclusif, c'est-à-dire telle que :

$$\forall (x,y): f(x \oplus y) = f(x) \oplus f(y)$$

C'est le cas, entre autres, des permutations et du transfert de données.

Comme mentionné précédemment, un DES classique se compose d'opérations répondant aux critères définis ci-dessus mais l'invention s'applique aussi à tout algorithme remplissant une fonction analogue à celle d'un DES, pourvu qu'il soit constitué d'opérations remplissant les conditions énoncées ci-dessus.

D'autres opérations à caractère aléatoire peuvent être combinées à celles qui définissent le procédé décrit ci-dessus. Notamment, lorsque plusieurs opérations consécutives de la chaîne sont commutatives, on peut permuter l'ordre de leur exécution, de façon aléatoire.

REVENDICATIONS

1- Procédé d'élaboration d'un protocole cryptographique entre une première entité électronique (A) et une seconde entité électronique (B) susceptible d'attaque, selon lequel un message quelconque (M) est élaboré, à partir duquel une chaîne d'opérations est effectuée par ladite seconde entité, aboutissant à l'élaboration d'un message résultant ou réponse (R), ladite réponse étant comparée au résultat d'un autre traitement semblable appliqué audit message et effectué par ladite première entité, caractérisé en ce que, au moins à certaines étapes de ladite chaîne d'opérations, ladite seconde entité effectue, soit une opération d'un type choisi (O_1, O_2, O_3 ... O_n), soit la même opération complémentée ($\overline{O_1}, \overline{O_2}, \overline{O_3}, \ldots \overline{O_n}$), le choix dépendant d'une décision aléatoire et en ce que ladite réponse est constituée par le résultat de la dernière opération ($\overline{O_n}$) de ladite chaîne, éventuellement complémenté.

2- Procédé selon la revendication 1, caractérisé en ce qu'une opération susceptible d'être complémentée est l'opération dite de OU exclusif.

3- Procédé selon la revendication 1 ou 2, caractérisé en ce qu'une opération susceptible d'être complémentée est une opération de permutation des bits dudit message ou d'un résultat intermédiaire obtenu en effectuant ladite chaîne d'opérations.

4- Procédé selon l'une des revendications 1 à 3, caractérisé en ce qu'une opération susceptible d'être complémentée est l'opération d'accès indexé à un tableau.

5- Procédé selon l'une des revendications 1 à 4, caractérisé en ce qu'une opération susceptible d'être complémentée est une opération stable par rapport à l'application de la fonction OU exclusif.

6- Procédé selon la revendication 5, caractérisé en ce qu'une opération susceptible d'être complémentée est le transfert dudit message ou d'un résultat intermédiaire obtenu en effectuant une opération de ladite chaîne, d'un emplacement à un autre d'un espace de mémorisation.

7- Procédé selon l'une des revendications précédentes, caractérisé en ce qu'il consiste à utiliser ledit message ou un résultat intermédiaire résultant de

l'exécution d'une opération précédente de ladite chaîne, à lui appliquer une nouvelle opération de ladite chaîne, ou cette même opération complémentée, en fonction de l'état d'un paramètre aléatoire (S'_a) associé à cette nouvelle opération, à mettre à jour un compteur de complémentations (C_c) et à prendre en compte l'état de ce compteur à la fin de l'exécution de ladite chaîne d'opérations pour décider de la configuration finale de ladite réponse.

8- Procédé selon l'une des revendications 1 à 6, caractérisé en ce qu'il consiste à utiliser ledit message ou un résultat intermédiaire résultant de l'exécution d'une opération précédente de ladite chaîne, à lui appliquer une nouvelle opération de ladite chaîne, ou cette même opération complémentée, en fonction de l'état d'un paramètre aléatoire (S'_a) associé à cette nouvelle opération et à transmettre, d'opération en opération, des informations faisant partie desdits résultats intermédiaires, nécessaires à la configuration finale de ladite réponse.

9- Procédé selon l'une des revendications 1 à 6, caractérisé en ce qu'on définit dans ladite seconde entité deux chaînes d'opérations (Ch_1, Ch_2) pour le traitement dudit message, l'une des chaînes étant constituée d'une suite d'opérations données et l'autre chaîne étant constituée d'une suite des mêmes opérations complémentées et d'une complémentation finale (C) et en ce qu'on décide de façon aléatoire d'exécuter l'une des deux chaînes d'opérations à chaque élaboration d'un message précité.

10- Procédé selon l'une des revendications précédentes, caractérisé en ce que, pendant qu'on effectue ladite série d'opérations, on calcule la différence (d) entre le nombre de fois où les opérations ont été effectuées de façon normale et le nombre de fois où elles ont été effectuées avec complémentation et en ce qu'on supprime l'aléa (S'_a) sur la décision d'effectuer des opérations de façon normale ou complémentée, pour exécuter un certain nombre d'opérations subséquentes, lorsque ladite différence dépasse une valeur prédéterminée dans le mode (normal ou complémenté) le moins utilisé jusque là, en vue de réduire suffisamment ladite différence.

11- Procédé selon l'une des revendications précédentes, caractérisé en ce que la complémentation est effectuée octet par octet.

12- Procédé selon l'une des revendications 1 à 10, caractérisé en ce que la complémentation est effectuée bit à bit.

13- Procédé selon l'une des revendications précédentes, caractérisé en ce que, lorsque plusieurs opérations consécutives de ladite chaîne sont commutatives, on permute l'ordre de leur exécution, de façon aléatoire.

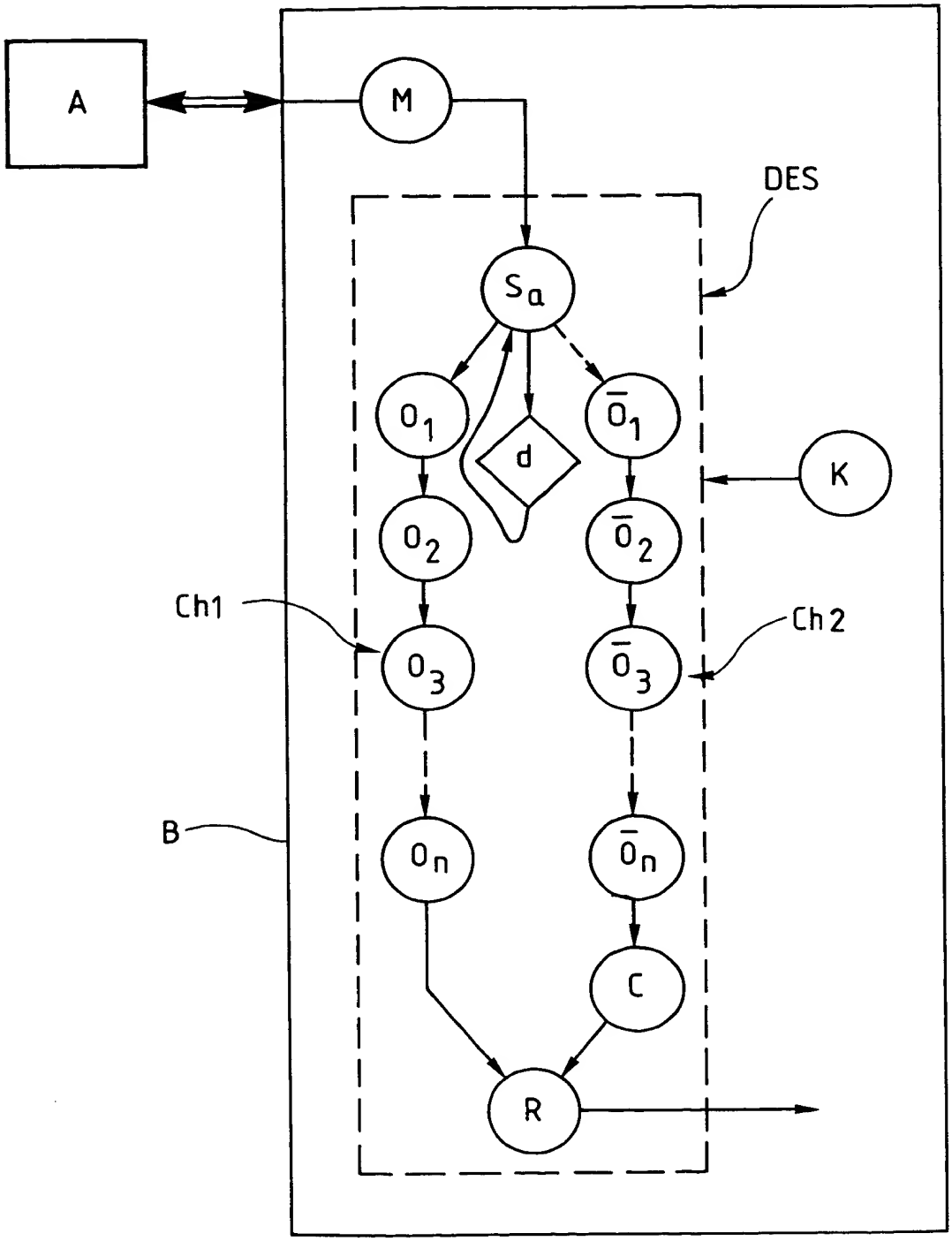

Fig.1

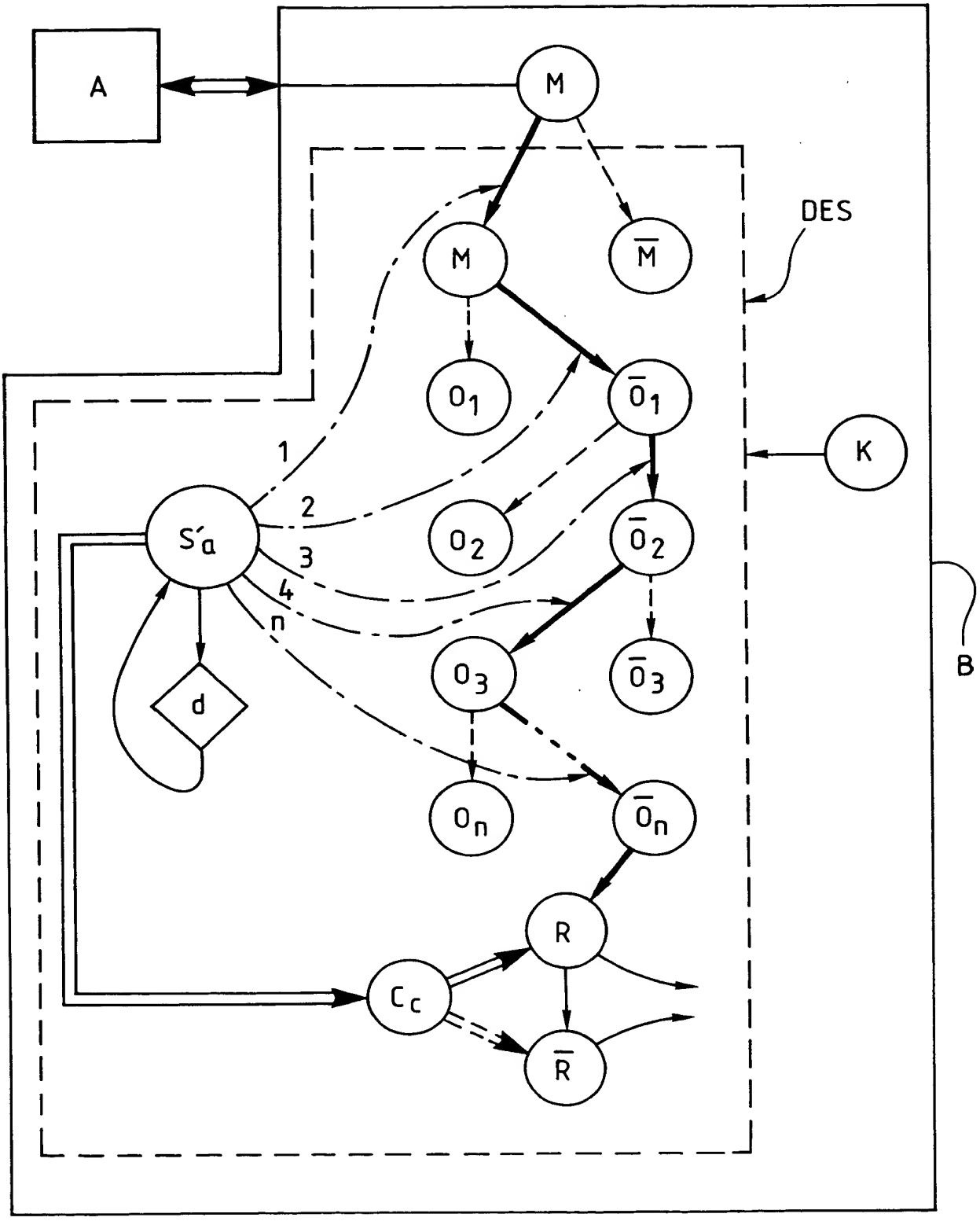
A
M
M
$\overline{M}$
DES
O_1
$\overline{O}_1$
K
1
2
S'a
O_2
$\overline{O}_2$
3
4
n
B
O_3
$\overline{O}_3$
d
O_n
$\overline{O}_n$
R
C_c
$\overline{R}$

Fig. 2